Passive Covert Radars using CP-OFDM SFN. Reference signal recovery from blind beamforming

Ghislain Gassier, Francoise Briolle, Gilles Chabriel, Jean Barrère

Passive Covert Radars using CP-OFDM SFN. Reference signal recovery from blind beamforming

Ghislain Gassier*, Francoise Briolle †,Gilles Chabriel *, Jean Barrère *
*UTLN, CNRS-IM2NP, Bat. R, BP 132, F-83957 La Garde Cedex, France
Email: ghislain.gassier@im2np.fr, gilles.chabriel@im2np.fr, jean.barrere@im2np.fr
† Aix Marseille Université, Université de Toulon, CNRS, CPT, UMR7332, 13288 Marseille, France
Email: briolle@cpt.univ-mrs.fr

***Abstract*—A passive Coherent Location (PCL) system uses the signal transmitted by so called illuminators-of-opportunity in the environment for the illumination of targets. It is then necessary to recover the original transmitted signal to be compared to the targets echoes. With CP-OFDM transmissions, it is quite easy to recover the original data and then to reconstruct the original transmission. But in the case of a Single Frequency Network , characterized by the presence of several transmitters using the same carrier frequency to broadcast the same signal, it is necessary to use directional sensors or spatial filter. In this paper, we propose two blind solutions : classical beamforming and CAPON filtering. Results of real measurements are presented.**

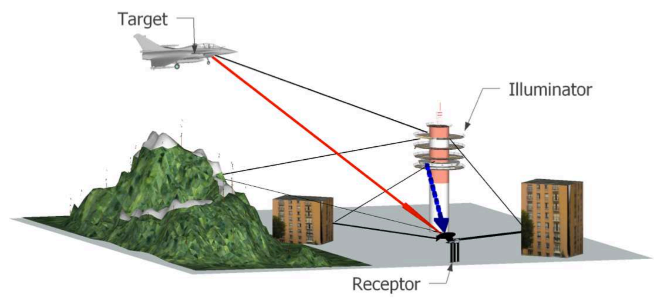

Fig. 1: Passive radar scene.

I. Introduction

A passive Coherent Location (PCL) system or Passive Covert Radar is an emerging and highly promising technology, which may be used in many application areas in the future [1], [2], [3], [4].

A passive radar exploits the availability of so called illuminators-of-opportunity in the environment for the illumination of targets. The illuminators, normally used for radio or TV broadcasting, GSM transmissions, Wifi, etc. could be associated to a Passive Covert Radar [5], [6], [7]. The key-benefits of passive radar are, apart from its covert operation, the low-cost nature due to saving on expensive transmitters as well as detection of low-altitude and/or stealthy targets.

A. Context

A typical Passive Covert bi-static Radar scene is illustrated in Fig. 1, where a standard transmitter illuminates a scene composed of different static reflectors due to topography, to buildings, ..., and one or several moving targets (here an aircraft). A receiving antenna collects the radiations from the transmitter (direct path) and from the different reflectors.

Usually, a passive radar is equipped with two receiving channels: reference and surveillance channels. The signal from the reference channel, is used as the original transmitted signal (direct path) and compared to the surveillance signal.

Nowadays broadcast transmissions are changing more and more from analogue to digital. With CP-OFDM signals, used for Digital Audio and Video Broadcasting , Wifi transmissions, etc., it is possible to recover the transmitted digital data and then, to synthesize a sampled version of the original transmitted signal. The main difficulty of such a system will be first, to extract from the surveillance signal the only direct path and second, the very weak targets echoes. The direct path, used as a reference signal, will be compared to the target echoes in order to estimate the delay and the doppler effect.

After a brief description of the structure and properties of the CP-OFDM signals (SEC II), we will recall the main steps to process the demodulation of the signal in order to recover the original transmitted data (SEC III). The single-frequency network (SFN) broadcast is characterized by the presence of two or more transmitters using the same spectrum to broadcast the same signal. It is then necessary to use spatial filtering to recover the original data. Two spatial filters will be elaborated and results on real data will be presented in SEC IV.

II. CP-OFDM signals

The analog CP-OFDM signal is a sequence of OFDM blocks of duration T_s ; the structure of each OFDM block relies on an orthogonal frequency division multiplexing (OFDM), which consists in a modulation method of orthogonal sub-carriers.

Each OFDM block is composed of two parts : the useful part of duration T_u and a redundant part of duration T_{cp}, called the cyclic prefix (CP).

The useful part of the OFDM block $\#m$ is composed of K orthogonal sub-carriers f_k carrying a complex data d_k^m which can only take M different numerical complex values, depending on the M-array QAM modulation used. Note

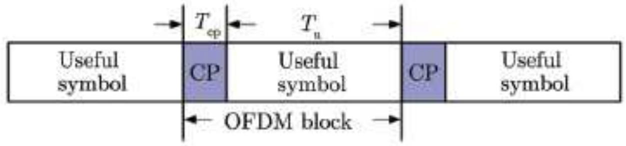

Fig. 2: Structure of a CP-OFDM block.

that orthogonality (on the duration T_u) between any pair of sub-carriers requires that $f_k = \frac{k}{T_u}$.

The cyclic prefix (CP) is obtained by copying the last part of the block and attaching it in front of the useful part. The duration T_{cp} of the cyclic prefix is usually assumed to be greater than or equal to the delays of the echoes ; then, it allows to eliminate inter blocks (ISI) and inter carrier (ICI) interferences.

Assuming that the emitter time origin is taken at the emission of the first OFDM block ($m = 0$), we can express, in baseband, the m^{th} emitted OFDM block as:

$$d^m(t) = \sum_{k=0}^{K-1} d_k^m \exp(2i\pi \tfrac{k}{T_u} t) \quad mT_s < t \leq (m+1)T_s.$$

And the direct path (the reference signal), sequence of blocks

$$d(t) = \sum_{m=0}^{M} d^m(t),$$

Then, the signal $d(t)$ is upconverted using the carrier frequency F_0 and the transmitter sends $d(t)e^{2i\pi F_0 t}$.

The main advantage of CP-OFDM communication technique is its ability to deal with multipath propagation without complex equalization filters. We will detail the process to recover the digital data $\{d_k^m\}$ from the mixture received on the antenna of the passive radar.

III. CP-OFDM Demodulation

The signal from the surveillance channel is a mixture of the original transmitted signal (direct path) and echoes from static reflectors and moving targets, corrupted by sensor noise (Fig. 1). In baseband, this signal can be written as :

$$\begin{aligned} s_{surv}(t) =& \Big(A\, d(t-t_0) + \sum_i \alpha_i\, d(t-t_0-\tau_i) \\ &+ \sum_j \beta_j\, d(t-t_0-\tau_j)\, e^{i2\pi f_j^d t} \Big)\, e^{2i\pi F_0 t} + \eta(t) \end{aligned} \tag{1}$$

where

- t_0 is the propagation delay between the receiving antenna and the transmiter,
- $\tau_i + t_0$ and $\tau_j + t_0$ are the delays between the receiving antenna and respectively the i^{th} static reflector and the j^{th} target,
- f_j^d is the frequency shift due to the radial velocity of the target j (Doppler effect),
- A, α_i, β_j are complex factors. α_i and β_j are related to positions and radar cross section (RCS) of the different reflectors.
- $\eta(t)$ is the sensor noise contribution assumed to be centered.

Let denote $d_{ref}(t)$ the reference signal, proportional and delayed version of $d(t)$, the surveillance signal can be written as:

$$\begin{aligned} s_{surv}(t) =& \Big(d_{ref}(t) + \sum_i a_i d_{ref}(t-\tau_i) \\ &+ \sum_j b_j\, d_{ref}(t-\tau_j)\, e^{i2\pi f_j^d t} \Big)\, e^{2i\pi F_0 t} + \eta(t). \end{aligned}$$

A. Process

The process to synthesize a sampled version of the reference signal $d_{ref}(t)$ performs the following 7 steps :

1) Baseband downconversion
The surveillance signal $s_{surv}(t)$ is analogically multiplied by $e^{-2i\pi F_0^R t}$ to get the signal in the baseband:

$$\begin{aligned} x_{surv}(t) = & \Big(d_{ref}(t) + \sum_i a_i\, d_{ref}(t-\tau_i) \\ &+ \sum_j b_j\, d_{ref}(t-\tau_j)\, e^{i2\pi f_j^d t} \Big)\, e^{2i\pi f_{CFO} t} + \eta(t), \end{aligned}$$

where $f_{CFO} := F_0^R - F_0$ is the carrier frequency offset (CFO) between the transmitter and the receiver local oscillators. A method to estimate the CFO can be found e.g. in [8].

2) Sampling
The duration of each OFDM block is $T_s = N_s.\Delta$, with Δ the sampling period, given by the CP-OFDM standard. We consider here that the sampling frequency offset (SFO) effect is negligible. However, some estimation and correction methods can be found in [8], [9], [10]. If we assume that $\tau_k = n_k \Delta$ is an integer multiple of the sampling period, then the sampled surveillance signal yields

$$\begin{aligned} x_{surv}(n) = & \Big(d_{ref}(n) + \sum_i a_i\, d_{ref}(n-n_i) \\ &+ \sum_j b_j\, d_{ref}(n-n_j)\, e^{i2\pi f_j^d n} \Big)\, e^{2i\pi f_{CFO} n} + \eta(n). \end{aligned}$$

3) Synchronization
The goal of this synchronization is to detect the beginning of a CP-OFDM block.
Each CP-OFDM block is composed of K orthogonal sub-carriers. P of them, called pilots frequencies, carry a specific value $\{d_p\}$. The values and the frequencies $\{f_p\}$ of the pilots are given by the DVB-T standard. The synthesized sampled time sequence of pilots, over N OFDM blocks, is

$$x_P(n) = \sum_{p=1}^{P} d_p e^{2i\pi f_p n} \quad n = 1 \ldots N.N_s \,,$$

Nota : The DVB-T norm imposes that the frequencies of some pilots (continual and TPS) are the same for all OFDM blocks. The frequency of scattered pilots differs from one block to another, with a periodicity of four blocks. Here, for simplicity, this detail is omitted (see [**?**]).

The position m_0 of the first peak of the intercorrelation sequence between the sampled surveillance signal $x_{surv}(n)$ and the sequence of pilots $x_P(n)$ gives the position of the first OFDM block.

Then, the surveillance signal can be written as a sequence of N OFDM blocks, with the block $\#m$

4) Equalization

For each OFDM block, the cyclic prefix will be removed. The block $\#m$ is equal to

$$x_{surv}^m(n) = \sum_{k=0}^{K-1} \tilde{d}_k^m e^{2i\pi \frac{k}{T_u} n},$$

where $\tilde{d}_k^m = H^m(\frac{k}{T_u}) d_k^m$ is the complex amplitude of the k^{th} sub-carrier. This value can be easily obtained by Inverse Fast Fourier Transform.

The values $\{d_p^m\}$ of the pilots are known, and the frequency response of the propagation channel is known for the pilots frequencies $\{f_p^m\}$

$$H^m(f_p^m) = \frac{d_p^m}{\tilde{d}_p^m}$$

The frequency response of the propagation channel, $H(\frac{k}{T_u})$ for $k \neq p$, is obtained by linear interpolation. Then, an estimation of the transmitted data can be obtained by equalization,

$$d_k^m = \tilde{d}_k^m \times H(\frac{k}{T_u}). \tag{2}$$

This equalization will be done for each block. Figures 6 or 7 show the real part versus the imaginary part (constellation diagram) of the equalized data $\{d_k\}$ for N OFDM blocks. We can note here that the data $\{d_k\}$ take only 16 different complex values plus 4 real values used for the pilots.

5) CFO correction

The continual and TPS pilots have the same frequency f_p for each OFDM block. The Carrier Frequency Offset will be estimated by the phase shift of data pilots through N OFDM blocks. The average phase shift for 60 OFDM blocks is plotted on figure 3. A linear regression estimation will give the slope S of the line and the estimation of $f_{CFO} = \frac{S}{2\pi}$. Multiplying the $x_{surv}(n)$ by $e^{-2i\pi f_{CFO} n}$ will correct the CFO effect.

Then after correction, the equalization process will be done again as it is described above.

6) Mapping

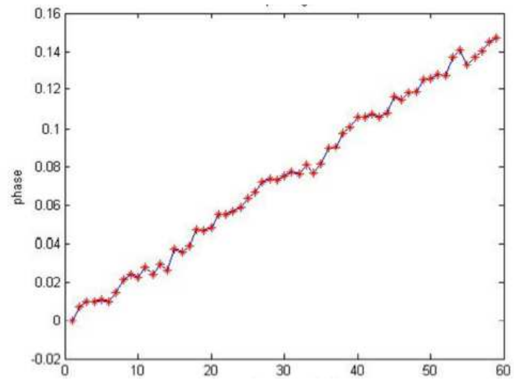

Fig. 3: Average of the phase shift fover 60 OFDM blocks

The binary flow was encoding with a 16-QAM. We have then to map the equalized set $\{d_k\}$ to 16 complex values plus 4 real ones to obtain the original transmitted data.

7) Reconstruction of the reference signal

From the original transmitted data set,the sampled useful part, of duration T_u, is obtained by FFT for each OFDM block. Then by copying the last part and attaching it in front, we will reconstruct the OFDM block of duration T_s.

IV. Demodulation in SFN network configuration: results on real measurments

A. Context

A single-frequency network (SFN) is a broadcast network characterized by the presence of several transmitters using the same carrier frequency to broadcast simultaneously a same signal.

The campaign of measurements, we present, uses three DVB-T SFN illuminators (8K-mode, 514 MHz). The receiver is an array composed of 16 sensors. The positions of the different illuminators and the receiver are described on figure 4.

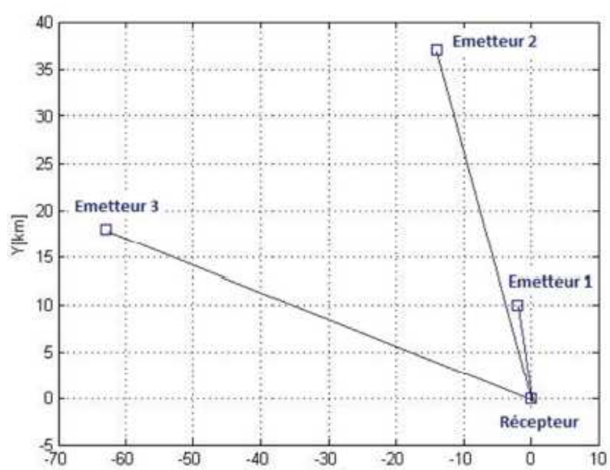

Fig. 4: Positions of the illuminators and the PCL receiver.

The direct path of the illuminator $\#1$ is followed by the strong direct paths of the illuminators $\#2$ then $\#3$, which can be seen as "strong echoes".

B. Modelling

With P transmitters in the SFN, the surveillance signal, can be modelled as

$$s_{surv}(t) = \Big(\sum_{p=1}^{P} A_p\, d(t - t_p) + (\sum_{p=1}^{P} \sum_{i} \alpha_{p,i}\, d(t - \tau_{p,i}) + \sum_{p=1}^{P} \sum_{j} \beta_{p,j}\, d(t - \tau_{p,j} t) e^{i2\pi f_{p,j}^{d} t} \Big) e^{2i\pi F_0 t} + \eta(t)$$

where $d(t-t_p)$ is the direct-path signal of p-th transmitter and A_p the corresponding complex amplitude; $\alpha_{p,i}$ and $\beta_{p,j}$ are the complex amplitude of static reflectors and the targets echoes and $\tau_{p,i}$ and $\tau_{p,j}$, the delays.

Here, the signal of interest (the mos powerful) is the direct path from the nearest transmitter, called the reference signal. Then the surveillance signal, after baseband downconversion, can also be written as,

$$x_{surv}(t) = \Big(d_{ref}(t) + \sum_{i,j} a_i d_{ref}(t - \tau_i) + d_{ref}(t - \tau_j) e^{i2\pi f_j^d t} \sum_{p=2}^{P} A_p d(t - t_p) + \sum_{i,j} \alpha_{p,i} d(t - \tau_{p,i}) + \beta_{p,j} d(t - \tau_{p,j} t) e^{i2\pi f_{p,j}^{d} t} \Big) e^{2i\pi f_{CFO} t} + \eta(t).$$

The main issue, when SFN illuminators are considered is that the P "strong echoes" due to these different transmitters produce a deep modulated channel frequency response so that the interpolation process fails.

Thanks to the CP-OFDM structure of the DVB-T signals, the synchronization can still be achieved by correlation with a pilot sequence. But if any spatial process is done to enhance the direct path from the nearest transmitter, then it will be impossible to recover the original data interpolating the pilot-free frequencies. The results (Fig. 5) are obtained when a single sensor is considered.

C. Spatial blind enhancement

The goal is here to enhance the signal emitted from the nearest transmitter.

Let us consider

- $\{x_{surv}^1(n), \dots x_{surv}^M(n)\}$, the surveillance signals recorded on the M sensors of the antenna,
- $\mathbf{x_s}$, the observations vector, $\mathbf{x_s} = [x_{surv}^1(n), \dots x_{surv}^M(n)]^T$,
- $\mathbf{R_x}$ spatial covariance matrix of the observations, $\mathbf{R_x} = \mathbf{x_s}.\mathbf{x_s}^H$.

To enhance the signal from the direction of arrival (DOA) θ_1 corresponding to the nearest transmitter, we have to estimate the steering vector $\mathbf{d}(\theta_1)$. For example, when a uniform (sensors equally spaced) linear antenna is considered, it is well known that the steering vector yields

$$\mathbf{d}(\theta_1) = [1, e^{2i\pi u(\theta_1)}, \dots, e^{2i\pi(M-1u(\theta_1))}]$$

where $u(\theta_1) = l\sin(\theta_1)/\lambda$, l is the distance between two adjacent sensors and λ the wavelength corresponding to the carrier frequency.

We show in the full paper that this steering vector can be blindly (without any geometrical or DOA consideration) estimated using both the sequence of pilots $x_P(n)$ used for the synchronization and the synchronized surveillance signals $x_{surv}^m(n)$. We show in particular that $\mathbf{d}(\theta_1)$ can be estimated using

$$\tilde{\mathbf{d}}(\theta_1) = \left[1, \frac{\Gamma_2(0)}{\Gamma_1(0)} \dots, \frac{\Gamma_M(0)}{\Gamma_1(0)}\right]^T$$

where $\Gamma_m(0) := \mathtt{E}\{x_P^*(n) x_{surv}^m(n)\}$.

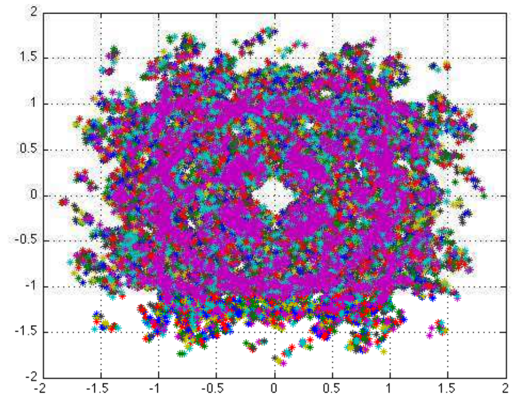

Fig. 5: Constellation diagram of the equalized data (without any spatial processing)

Now, from this estimated steering vector corresponding to the nearest transmitter, one can implement a spatial filtering in order to produce a beam where the contribution of the strong echoes due the presence of the other transmitters is reduced. In this study, we consider two different spatial filters $\mathbf{w}(\theta_1)$:

- The classical beamformer:

$$\mathbf{w}_{CB}(\theta_1) = \tilde{\mathbf{d}}(\theta_1)$$

- The CAPON beamformer:

$$\mathbf{w}_{\mathbf{CAPON}}(\theta_1) = \frac{\mathbf{R_x}^{-1}\tilde{\mathbf{d}}(\theta_1)}{\tilde{\mathbf{d}}(\theta_1)^H \mathbf{R_x}^{-1}\tilde{\mathbf{d}}(\theta_1)}$$

The two following figures shows the constellation diagrams obtained with the different spatial filters before the mapping step. One can see that in particular with the CAPON filtering, the quality of the obtained constellation is sufficiently good so that the last mapping process conducts to a perfect reference signal recovery. These figures have to be compared with Figure 5 where no spatial processing was implemented.

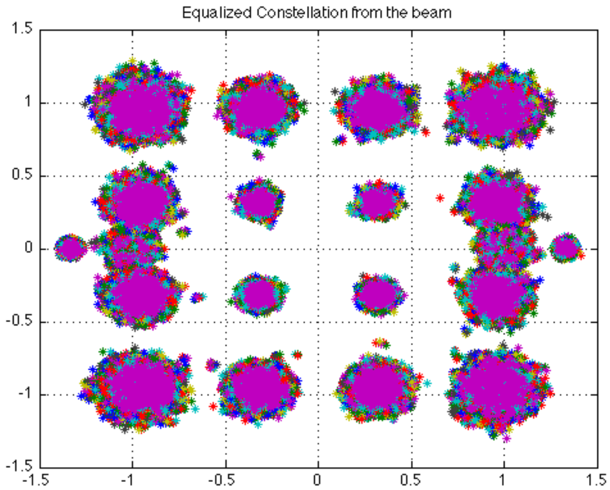

Fig. 6: CB-equalized data constellation diagram (0.4 Hz CFO compensation)

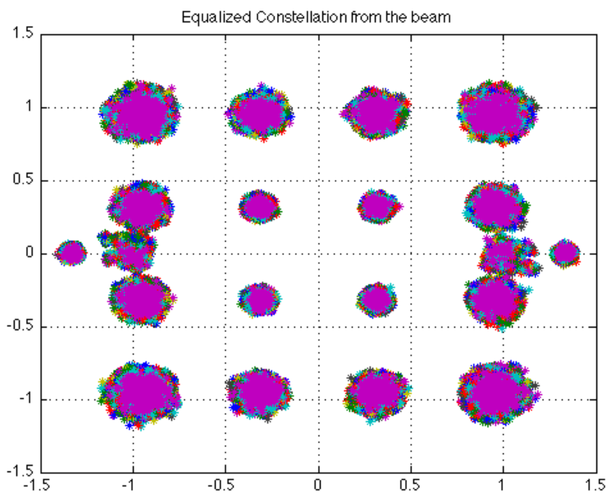

Fig. 7: CAPON-equalized data constellation diagram (0.4 Hz CFO compensation)

V. Conclusion

The Single Frequency Network broadcast is used in many countries : Germany, North of Europe, China, etc.. For such a network, the reference signal recovery needs a spatial processing. Two solutions were implemented : classical beamforming and spatial CAPON filter with a blind estimation of the steering vector of interest. The results obtained with real data indicate that the CAPON filter gives better results; the constellation diagram of the estimated data exhibits a satisfactory variance. Now, the computation of such a filter requires many operations while the implementation of classical beamforming is quite simple.

The main advantages for the Passive Coherent Location using CP-OFDM in a SFN mode is to have the targets illuminated by several transmitters. It is then possible to localize accurately the targets.

Acknowledgment

The campaign of measurements was achieved by Thales Air Systems, ONERA, DGA (Direction Générale de l'Armement) and CEAM (Centre d'Expériences Aériennes Militaires) jointly with the BWB (Bundesamt fr Wehrtechnik und Beschaffung) and Fraunhofer Institute. We are particularly grateful to J. Colin, from the DGA, for giving us access to the data.

References

[1] H. Kuschel and D. O'Hagan,*Passive radar from history to future*, in Radar Symposium (IRS), 2010 11th International (pp. 1-4). IEEE, 2010.

[2] J.M. Thomas, C.J. Baker and H.D. Griffiths, *HF passive bistatic radar potential and applications for remote sensing*, in New Trends for Environmental Monitoring Using Passive Systems, 2008 (pp. 1-5). IEEE, 2008.

[3] J. Song, Y. He, F.Q Cai, and X.M. Tang, *Overview of passive radar technology based on non-cooperative radar illuminator*. Systems Engineering and Electronics, 31(9), 2151-2156, 2009.

[4] H.D. Griffiths, and C.J. Baker, C. J. *Passive coherent location radar systems. Part 1: Performance prediction* in Radar, Sonar and Navigation, IEE Proceedings- Vol. 152, No. 3, pp. 153-159. IET, 2005.

[5] P. Falcone, F. Colone, C. Bongioanni, C.and P. Lombardo, *Experimental results for OFDM WiFi-based passive bistatic radar* in Radar Conference, 2010 IEEE (pp. 516-521). IEEE, 2010.

[6] H. Sun, D.K. Tan,Y. Lu, and M. Lesturgie, *Applications of passive surveillance radar system using cell phone base station illuminators*. Aerospace and Electronic Systems Magazine, IEEE, 25(3), 10-18, 2010

[7] X. Neyt,J. Raout, M. Kubica, V. Kubica, S. Roques, M. Acheroy, M. and J.G. Verly, *Feasibility of STAP for passive GSM-based radar* in Radar, 2006 IEEE Conference on (pp. 6-pp). IEEE, 2006.

[8] M. Sliskovic, *Carrier and sampling frequency offset estimation and correction in multicarrier systems*, in Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE, Vol. 1, pp. 285-289, 2001

[9] E.S Shim, S.T Kim, H. K. Song, and Y. H. You, *OFDM carrier frequency offset estimation methods with improved performance*, Broadcasting, IEEE Transactions on, 53(2), pp. 567-573, 2007

[10] Y.H. You, S.T. Kim, K.T. Lee, and H.K. Song, *An improved sampling frequency offset estimator for OFDM-based digital radio mondiale systems*, Broadcasting, IEEE Transactions on, 54(2), pp. 283-286, 2008.